REMARKS

Claims 21-28 are pending, with claim 21 being independent. Reconsideration and allowance of the above-referenced application are respectfully requested.

Rejections under 35 U.S.C. 103

Claims 21-28 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Kouznetsov (U.S. Patent 6,973,577), and further in view of Gryaznov (U.S. Patent 7,065,790). This contention is respectfully traversed.

Claim 21 recites, in part, "one or more machines coupled with the network, each machine comprising a communication interface and a memory including an execution area configured to perform operations comprising examining a set of instructions embodying an invoked application to identify the invoked application, obtaining application-specific intrusion criteria, and monitoring network communications for the invoked application, after the examining and the obtaining, using the application-specific intrusion criteria to detect an intrusion." Kouznetsov fails to teach or suggest the claimed subject matter, either alone or in combination with Gryaznov.

Kouznetsov teaches a system and a method for dynamically detecting computer viruses through associative behavioral analysis of runtime state.[1] But Kouznetsov does not in any way teach obtaining application-specific intrusion criteria. In rejecting this claimed feature, the

---

[1] *See* Kouznetsov at Abstract.

Office cites to, and underlines, a portion of Kouznetsov that <u>does not</u> describe <u>application-specific intrusion criteria</u>[2]:

> The sequence of the execution of the monitored events is tracked for each of the applications. <u>Each occurrence of a specific event sequence characteristic of computer virus behavior and the application that performed the specific event sequence, are identified. A histogram describing the specific event sequence occurrence for each of the applications is created.</u> Repetitions of the histogram associated with at least one object are identified.
>
> The process identifier (ID) 71 and application name 72 fields respectively store the process number and name of the application 33, 34, 35 (shown in FIG. 2) to which the recorded monitored event is associated.
>
> ... records for the monitored events 70 are retrieved for each of the applications 33, 34, 35 (block 151).

The Office then states[3]:

> The underlined citation above reads on the claimed application-specific intrusion criteria that were tracked for each application as monitored events. Applicant later acknowledges on pg.6, that (col.2, lines 51-58 and col.5, lines 9-12 and col.7, lines 1-2)the monitored events are then analyzed to determine whether the application is performing a sequence of suspicious actions characteristic of computer viruses (col.2, lines 32-40 and col.4, lines 15-36). This clearly shows obtaining intrusion criteria that are specific to an application.

This is <u>not</u> correct. A "specific event sequence characteristic of computer virus behavior", as described in Kouznetsov, <u>does not</u> constitute intrusion criteria, but rather is the output of the tracking performed using intrusion criteria.

---

[2] *See* Kouznetsov at col. 2, lines 51-58 and col. 5, lines 9-12 and col. 7, lines 1-2; and 12-10-2008 final Office Action at p. 2.

[3] *See* 12-10-2008 final Office Action at p. 2.

This misconception by the Office can be clearly seen by looking at the Office's statement that, "The underlined citation above reads on the claimed application-specific <u>intrusion criteria that were tracked</u> for each application as monitored events."[4] Attention is called to the fact that the present claims <u>do not</u> state that <u>intrusion criteria</u> are tracked. To the contrary, the present claims specify that network communications for the invoked application are monitored using the application-specific intrusion criteria.

Far from teaching the use of application-specific intrusion criteria, Kouznetsov actually teaches the opposite. Kouznetsov teaches that the program state of the executing applications is monitored by a monitor/analyzer 19 that monitors all applications equally using apparently common criteria[5]:

> The program state of the executing applications 33, 34, 35 is monitored by the monitor/analyzer 19 that generates histograms based on occurrences of monitored events. The monitor/analyzer 19 functions as a logical "shim" interposed between the operating system 32 and each of the applications 33, 34, 35. Each system call is intercepted by the monitor/analyzer 19 which compares the requested system call to a list of monitored events. If the system call matches one of the monitored events, the monitor 19 determines whether the application is performing a sequence of "suspicious" actions characteristic of computer viruses. If so, histograms of the event occurrences are generated and stored in a database 37 maintained in the storage device 36.

Nothing here, or in any other part of Kouznetsov, suggests that this determination of whether the application is performing a sequence of "suspicious" actions characteristic of computer viruses is based on criteria specific to an application. Rather, Kouznetsov merely states that when a suspicious event sequence is identified, the application performing that event sequence is also

---

[4] *See* 12-10-2008 final Office Action at p. 2; emphasis added.
[5] *See* Kouznetsov at col. 4, lines 15-27.

identified. Thus, Kouznetsov does not in any way teach the claimed, "obtaining application-specific intrusion criteria" and "monitoring network communications for the invoked application [...] using the application-specific intrusion criteria to detect an intrusion." On this basis alone, all of the current rejections should be withdrawn.

In addition, neither Kouznetsov nor Gryaznov, either alone or in combination, teaches or suggests, "examining a set of instructions embodying an invoked application to identify the invoked application", as claimed. The cited portions of Kouznetsov teach traditional loading and executing of program code.[6] Interpreting the present claim language, "examining a set of instructions embodying an invoked application" as reading on the traditional loading and executing of program code is inconsistent with the present specification and is thus an improper claim construction under the law and the MPEP.[7] The Office has failed to address this point.

Moreover, the Office's use of Gryaznov in combination with Kouznetsov to address the full claim feature, "examining a set of instructions embodying an invoked application to identify the invoked application", is without merit. The Office has split this claim feature into two parts: (1) "examining a set of instructions embodying an invoked application", and (2) "to identify the invoked application"; and the Office then attempts to combine Gryaznov with Kouznetsov to arrive at the full claim feature. Gryaznov describes a method, system, and computer program product that provides multiple names of a given malware in a quick and automated fashion.[8] As noted above, and in sharp contrast, Kouznetsov teaches a system and a method for dynamically detecting computer viruses through associative behavioral analysis of runtime state. The Office has provided no logical reasoning with some rational underpinning to combine these two

---

[6] *See* Kouznetsov at col. 2, lines 47-48 and col. 4, lines 12-14 and 28-47.
[7] *See e.g.,* MPEP § 2111.01.
[8] *See* Gryaznov at Abstract.

references to support the legal conclusion of obviousness, as is required by law. The undersigned attorney has read the Response to Arguments section on this point multiple times and fails to grasp the Office's position. In particular, the Office appears to confuse the claimed "examining a set of instructions embodying an invoked application to identify the invoked application" with the "obtaining application-specific intrusion criteria",[9] and the Office fails to "identify the reason why a person of ordinary skill in the art would have combined the prior art elements in the manner claimed."[10] Thus, the current rejection suffers from a clear legal or factual deficiency.

In view of the above, independent claim 21 should be in condition for allowance. Dependent claims 22-28 should be patentable based on the above arguments and the additional recitations they contain. For example, claim 28 recites, "wherein examining the set of instructions comprises: applying a hash function to the set of instructions to generate a condensed representation; and comparing the condensed representation with existing condensed representations for known applications." The cited portion of Kouznetsov says nothing about applying a hash function to the set of instructions to generate a condensed representation, and the Office has provided no explanation of the basis for rejecting this claim.[11] Thus, the rejection of claim 28 suffers from a clear legal or factual deficiency for at least this additional reason.

---

[9] See 12-10-2008 final Office Action at pp. 2-3.

[10] See Memorandum dated May 3, 2007, to Technology Center Directors from Margaret A. Focarino, Deputy Commissioner for Patent Operations, re Supreme Court decision on KSR Int'l. Co., v. Teleflex, Inc. (emphasis added).

[11] See Kouznetsov at col. 5, lines 50-58; and 12-10-2008 final Office Action at p. 7.
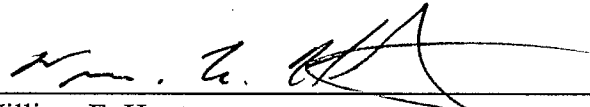
No fees are believed due with this response. Nonetheless, please apply any necessary

charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: _Feb. 9, 2009_

William E. Hunter
Reg. No. 47,671
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer No. 20985
Telephone: (858) 678-5070
Facsimile: (877) 769-7945

10892769.doc